UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

KIMBERLY HOOD, PATRICIA LADD, and SHARON FELTNER individually and on behalf of all others similarly situated, Plaintiffs, v. U.S. BANK NATIONAL ASSOCIATION and U.S. BANCORP, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Kimberly Hood, Patricia Ladd and Sharon Feltner ("Plaintiffs"), by and through their attorneys, bring this class action on behalf of themselves and all similarly-situated individuals against U.S. Bank National Association ("U.S. Bank"), and its parent company U.S. Bancorp ("U.S. Bancorp") (collectively, "Defendants").

INTRODUCTION AND NATURE OF ACTION

1. Plaintiffs bring this class action against Defendants U.S. Bancorp and U.S. Bank National Association ("Defendants" or "U.S. Bank") for their failure to secure and safeguard the confidential, personally identifiable information of thousands of consumers – including names, account numbers, Social Security numbers, driver's license numbers, and dates of birth ("PII").

2. Defendants provide banking, investment, mortgage, trust, and payment services products to individuals, businesses, governmental entities, and other financial institutions.

3. As of December 31, 2019, U.S. Bank was the fifth-largest bank in the country, with more than 70,000 employees and $495 billion in assets.

4. Defendants promised Plaintiffs and the Class members that Defendants would protect their PII. Defendants' "Privacy Pledge" states:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings[1].

5. Defendants did not live up to that promise. On or about July 30, 2020, and due to Defendants' wholly inadequate security and failure to comply with federal and state data privacy standards, a computer server containing an unknown quantity of business and/or consumer PII was physically taken from one of Defendants' corporate offices.

6. Due to Defendants' carelessness and inadequate security, Plaintiffs and Class members have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiffs' and Class members' PII has been compromised and they must now undertake additional security measures to minimize the risk of identity theft.

[1] https://www.usbank.com/about-us-bank/privacy/privacy-pledge.html

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

8. This Court has jurisdiction over Defendants because U.S. Bancorp maintains its principal place of business in Minnesota, and both Defendants regularly conduct business in Minnesota and have sufficient minimum contacts in Minnesota. Defendants intentionally avail themselves of this jurisdiction by marketing and selling products and services from Minnesota to millions of consumers nationwide, including in Minnesota.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant U.S. Bancorp's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

10. Plaintiff Kimberly Hood ("Plaintiff"), a resident of California, had her PII stolen and/or accessed and/or improperly utilized as a result of the U.S. Bank data breach on July 30, 2020. Plaintiff Hood's PII stored on the stolen U.S. Bank server was compromised in and because of the data breach. Plaintiff Hood was harmed by having her PII compromised. Plaintiff received notice that the subject information she had provided Defendants was no longer secure.

11. Plaintiff Patricia Ladd ("Plaintiff"), a resident of California, had her PII stolen and/or accessed and/or improperly utilized as a result of the U.S. Bank data breach on July 30, 2020. Plaintiff Ladd's PII stored on the stolen U.S. Bank server was compromised in and because of the data breach. Plaintiff Ladd was harmed by having her PII compromised. Plaintiff received notice that the subject information she had provided Defendants was no longer secure.

12. Plaintiff Sharon Feltner ("Plaintiff"), a resident of Michigan, had her PII stolen and/or accessed and/or improperly utilized as a result of the U.S. Bank data breach on July 30, 2020. Plaintiff Feltner's PII stored on the stolen U.S. Bank server was compromised in and because of the data breach. Plaintiff Feltner was harmed by having her PII compromised. Plaintiff received notice that the subject information she had provided Defendants was no longer secure. Following the data breach Plaintiff has incurred unauthorized charges on her U.S. Bank debit card.

13. Defendant U.S. Bancorp is an American bank holding company operating under the Bank Holding Company Act of 1956, and is based in Minneapolis, Minnesota, and incorporated in Delaware. It is the parent company of Defendant U.S. Bank National Association, the fifth largest banking institution in the United States.

14. Defendant U.S. Bank National Association is the banking subsidiary of U.S. Bancorp and has its principal place of business in Cincinnati, Ohio. As of December 31, 2019, U.S. Bank National Association had $374 billion in deposits.

FACTUAL BACKGROUND

15. As the fifth largest banking institution by assets in the United States, with revenues in the billions of dollars, U.S. Bank has both the duty and the financial wherewithal to provide for the physical security of its corporate offices and computer servers containing its clients' and customers' PII. Plaintiffs and Class members had a reasonable expectation that U.S. Bank would safely and securely store their PII from both physical and digital theft and misuse.

16. As detailed more fully below, however, U.S. Bank and its parent company U.S. Bancorp did not safely and securely store their PII from both physical and digital theft and misuse.

A. The Data Breach

17. On or about September 18, 2020, Defendants began notifying Plaintiffs and Class members their PII had been stolen. In its Notification Letter to customers about the breach, U.S. Bank stated:

> At U.S. Bank, we value your confidence in us and place the privacy and security of your information as a top priority. We are writing to let you know about an event that occurred at a U.S. Bank location, which included some of your personal information.
>
> **What happened:**
>
> On July 30, 2020, a computer server containing your information was physically stolen from one of our corporate offices. Since the event, we have been focused on identifying who was impacted and working with authorities to recover the stolen server.

18. The Notice also indicated the stolen PII "included personally identifiable information including your name, account number, Social Security number, driver's license number, and date of birth."

19. This incident is referred to herein as the "Data Breach."

20. Defendants' asserted commitment to privacy and security is belied by their failure to provide any specifics about the theft, their unreasonable delay in notifying Plaintiffs and the Class members of the breach, and their failure to offer sufficient affirmative steps to protect Plaintiffs' and the Class members' identities from theft.

21. This course of action is unfortunately not uncommon for Defendants. Just earlier this year, Defendants were taken to task for providing its customers a "cryptic" notice of data breach that was called "vague and deceptive" because it provided incomplete and potentially misleading information[2].

22. Not only are Defendants failing to disclose the complete nature of the breach, but they waited almost two months before notifying Plaintiffs and Class members that they may have been victims of data theft. This delay in notification to Plaintiffs and Class members gave the thieves time to use the stolen PII without restriction, further harming Plaintiffs and Class members.

[2] https://www.cincinnati.com/story/money/2020/02/11/fifth-third-data-breach-consumer-federation-america-slams/4722455002/

1. The Breach Was Entirely Avoidable and Foreseeable by Defendants.

23. Defendants could have prevented the data breach from occurring. Defendants failed to take adequate and reasonable measures to ensure their computer/server systems were protected against theft and failed to take actions that could have stopped the breach before it occurred.

24. Defendants failed to disclose to Plaintiffs and Class members that their computer/server systems and security practices were inadequate to reasonably safeguard customers' PII and failed to immediately notify its customers of the data theft.

25. As a direct result of Defendants' conduct, Plaintiffs and Class members were injured.

26. Defendants were at all times fully aware of their obligations under the law and various standards and regulations to protect data entrusted to it by consumers.

27. Despite Defendants' awareness of its data protection obligations, Defendants' treatment of the PII entrusted to it by its customers fell short of satisfying their legal duties and obligations. Defendants failed to ensure that access to their physical computer/server systems was reasonably safeguarded.

2. Data Breaches Lead to Identity Theft and Cognizable Injuries.

28. The personal and financial information of consumers, including Plaintiffs and Class members, is valuable.

29. The ramifications of Defendants' failure to keep Plaintiffs' and Class members' PII secure are severe. Identity theft occurs when someone uses another's

personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

30. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

31. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

32. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

33. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

34. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendants did not rapidly report to Plaintiffs and Class members that their PII had been stolen.

35. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

36. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

37. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[3] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[4]

38. Moreover, in light of the current COVID-19 pandemic, Plaintiffs' sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

---

[3] *See* Government Accountability Office, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited September 24, 2020).
[4] *Id.*

39. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

40. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

41. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class members will need to be remain vigilant against unauthorized data use for years or even decades to come.

42. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

43. Recognizing the high value consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information

they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[5]

44. Consumers place a high value on their PII, as well as on the privacy of their PII. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[6]

45. By virtue of the Data Breach and unauthorized release and disclosure of the PII of Plaintiffs and the Class, Defendants have deprived Plaintiffs and the Class of the substantial value of their PII, to which they are entitled. As previously alleged, contrary to their representations, Defendants failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

46. Defendants are aware of the potential harm caused by this data theft, stating: "We apologize for any inconvenience this has caused. As a precautionary measure, if you would like to receive a new account number, you can do so by calling our Fraud Liaison Center at 877.595.6256 between 8 a.m. to 9 p.m. CT, Monday through Sunday. We can help you close and reopen your account with a new account number at no charge."

---

[5] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, available at http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited September 24, 2020).

[6] *See* Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited September 24, 2020); *see also* Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

47. U.S. Bank's Notice Letter also states:

> [W]e recommend that you place a 'Fraud Alert' on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies, so you do not need to contact each of them separately….

48. According to the Federal Trade Commission ("FTC"), unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[7]

49. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

50. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

51. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once

---

[7] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited September 24, 2020).

used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

3. Plaintiffs and Class members Have Suffered Ascertainable Losses, Economic Damages and Other Actual Injury and Harm.

52. As a direct and proximate result of Defendants' wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and other Class members' PII, Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the untimely and inadequate notification of the Data Breach, (ii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and payment card accounts—for which they are entitled to compensation.

CLASS DEFINITION AND ALLEGATIONS

53. Plaintiffs bring this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

The Nationwide Class:

> All persons residing in the United States who had their U.S. Bank account information and/or other personal information compromised as a result of the Data Breach that occurred on or about July 30, 2020.

The California Subclass:

> All persons residing in the State of California who had their U.S. Bank account information and/or other personal information compromised as a result of the Data Breach that occurred on or about July 30, 2020.

Collectively, the Nationwide Class and the California Subclass with be referred to as "the Class" unless there is need to differentiate them. Excluded from the Class are: (i) Defendants and their officers, directors, affiliates, parents, and subsidiaries (ii) the Judge presiding over this action, and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads nolo contendere to any such charge.

54. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

55. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class include thousands of Defendants' customers who have been damaged by Defendants' conduct as alleged herein. The precise number of Class members is unknown to Plaintiffs but may be ascertained from Defendants' records.

56. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendants owed Plaintiffs and the other Class members a duty to adequately protect their PII;

d. whether Defendants breached their duty to protect the personal and financial data of Plaintiffs and the other Class members;

e. whether Defendants knew or should have known about the inadequacies of their data protection, storage, and physical property security;

f. whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class members' PII from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendants' offices and computer systems to safeguard and protect Plaintiffs' and the other Class members' PII from unauthorized theft, release or disclosure;

h. whether Defendants breached their promise in the Privacy Pledge to keep Plaintiffs and the Class members' PII safe and to follow federal data security protocols;

i. whether Defendants violated § 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and Class members' PII from unauthorized access and exfiltration, theft, or disclosure, as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;

j. whether Defendants' misconduct identified herein amounts to a violation of Cal. Bus. & Prof. Code § 17200, et seq.;

k. whether Defendants' conduct was the proximate cause of Plaintiffs' and the other Class members' injuries;

l. whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

m. whether Defendants' delay in informing Plaintiffs and the other Class members of the Data Breach was unreasonable;

n. whether Defendants' method of informing Plaintiffs and the other Class members of the Data Breach was unreasonable;

o. whether Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendants' conduct;

p. whether Plaintiffs and the other Class members are entitled to recover actual damages and/or statutory damages; and

q. whether Plaintiffs and the other Class members are entitled to other appropriate remedies, including injunctive relief.

57. Defendants engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

58. Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class members in the same manner.

59. Plaintiffs will fairly and adequately protect the interests of the members of the Class, has retained counsel experienced in complex consumer class action litigation, and intends to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

60. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

61. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

62. A special relationship exists between Defendants and the Plaintiffs and the Class. Defendants actively solicited Plaintiffs and the other Class members to use their PII in order to use Defendants' banking services and products. When Plaintiffs and the other Class members gave their PII to Defendants to facilitate those services, they did so with

the mutual understanding that Defendants had reasonable security measures in place and Defendants would take reasonable steps to protect and safeguard the PII of Plaintiffs and the other Class members. Indeed, Defendants explicitly represented that was the case. Plaintiffs and the other Class members also gave their PII to Defendants on the premise that Defendants had reasonable security measures in place and Defendants would take reasonable steps to protect and safeguard the PII of Plaintiffs and the other Class members. Plaintiffs and the other Class members also gave their PII to Defendants on the premise that Defendants were in a superior position to protect against the harm attendant to unauthorized access, theft, and misuse of that information.

63. Upon gaining access to the PII of Plaintiffs and members of the Class, Defendants owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed and misused by unauthorized parties. Pursuant to this duty, Defendants were required to design, maintain and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiffs and the Class. Defendants further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

64. Defendants owed this duty to Plaintiffs and the other Class members because Plaintiffs and the other Class members compose a well-defined, foreseeable and probable class of individuals whom Defendants should have been aware could be injured by Defendants' inadequate security protocols. Defendants actively solicited Plaintiffs and the

other Class members to use their PII when obtaining and utilizing banking services and products. To facilitate these banking services, Defendants used, handled, gathered and stored the PII of Plaintiffs and the other Class members. Attendant to Defendants' solicitation, use and storage, Defendants knew of their inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII that Defendants actively solicited, used and stored from Plaintiffs and the other Class members. As such, Defendants knew a breach of their systems would cause damage to their customers, including Plaintiffs and the other Class members. Thus, Defendants had a duty to act reasonably in protecting the PII of their consumers.

65. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and the other Class members the scope, nature and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the other Class members can take appropriate measures to avoid unauthorized use of their PII, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendants' unreasonable misconduct.

66. Defendants breached their duties to Plaintiffs and the other Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII of Consumer Plaintiffs and the other Class members.

67. Defendants also breached their duties to timely and accurately disclose to the

Plaintiffs and the other Class members that their PII had been or was reasonably believed to have been improperly accessed or stolen.

68. Defendants' negligence in failing to exercise reasonable care in protecting the PII of Plaintiffs and the other Class members is further evinced by Defendants' failures to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

69. The injuries to Plaintiffs and the other Class members were reasonably foreseeable to Defendants because laws and statutes, such as Minn. Stat. § 325E.64, and industry standards, such as the PCI DSS, require Defendants to safeguard and protect their computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class members' PII.

70. The injuries to Plaintiffs and the other Class members also were reasonably foreseeable because Defendants knew or should have known that their computer systems used for processing consumer sales transactions were inadequately secured and exposed consumer PII to being breached, accessed and stolen by hackers and unauthorized third parties. As such, Defendants' own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class members.

71. Defendants' failure to take reasonable steps to protect the PII of Plaintiffs and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the other Class members' PII. This ease of access allowed thieves to steal PII of Plaintiffs and the other members of the Class, which could lead to dissemination in black markets.

72. As a direct proximate result of Defendants' conduct, Plaintiffs and the other Class members have suffered theft of their PII. Defendants allowed thieves access to Class members' PII, thereby decreasing the security of Class members' bank accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Plaintiffs and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

73. Defendants' conduct warrants moral blame because Defendants actively solicited, used, handled and stored the PII of Plaintiffs and the other Class members without disclosing that their security was inadequate and unable to protect the PII of Plaintiffs and the other Class members. Holding Defendants accountable for their negligence will further the policies embodied in such law by incentivizing larger financial institutions to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Nationwide Class)

74. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

75. In engaging in the negligent acts and omissions as alleged herein, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect their customers' PII.

76. Defendants violated Section 5 by not complying with industry standards and

continually failing to have proper measures in place to protect the PII of Plaintiffs and the Class members.

77. Plaintiffs and the Class members are among the class of persons Section 5 was designed to protect, and the injuries suffered by Plaintiffs and the Class members is the type of injury Section 5 was intended to prevent. As a result, Defendants are negligent *per se*.

78. As a result of Defendants' negligence *per se*, Plaintiffs and the Class members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

79. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

80. Plaintiffs and Class members entered into an implied contract with Defendants by providing their PII to Defendant when using financial services provided by Defendants. Implied in these exchanges was a promise by Defendants to implement reasonable procedures and practices to protect the PII of Plaintiffs and Class members and to timely notify them in the event their PII was compromised.

81. Plaintiffs and Class members reasonably expected that Defendants had implemented adequate security measures to protect their PII and would allocate a portion of the money paid by Plaintiffs and Class members under the implied contracts to fund those security measures.

82. Neither Plaintiffs nor Class members would have provided their PII to Defendants or paid the same fees to Defendant for services without the implied contract

between them and Defendants. Defendants needed to adequately safeguard Plaintiffs' and Class members' PII and provide timely notice of a data breach to realize the intent of the parties.

83. Plaintiffs and Class members performed their obligations under the implied agreements with Defendants. Conversely, Defendants breached their obligations under the implied contracts by (i) failing to implement reasonable security procedures and practices to protect Plaintiffs' and Class members' PII; (ii) enabling unauthorized access of PII by third parties due to the inadequate security measures; and (iii) failing to provide timely notice of the Data Breach.

84. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiffs and Class members did not get the benefit of their implied contract with Defendants and were injured as described in detail above.

FOURTH CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class)

85. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

86. Defendants knew of or should have known that the PII Plaintiffs and Class members PII provided was highly confidential and sensitive.

87. Defendants' Privacy Policy is an agreement between Defendants and customers who provide PII to Defendants, which includes Plaintiffs and Class members.

88. Customers, including Plaintiffs and Class members, give certain PII to Defendants when they use Defendants' website and use Defendants' services. Plaintiffs and Class members therefore demonstrated their willingness and intent to enter into a

bargain with Defendants and assent to the terms of the Privacy Policy by giving their PII to Defendants.

89. Defendants demonstrated their intent to adhere to their obligations under the Privacy Policy and related statements when collecting Plaintiffs' and Class members' PII, including assuring customers that, "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."

90. Plaintiffs and Class members therefore entered into a contract with Defendants when providing PII to Defendants subject to the terms of the Privacy Policy.

91. Plaintiffs and Class members have upheld their obligations under the agreement. Defendants, on the other hand, breached their obligations by failing to implement reasonable security measures – specifically, failing in their promise of providing "secured files and buildings" – which led to unauthorized disclosure of PII to third parties.

92. As a direct and proximate result of Defendants' breach of this agreement, Plaintiffs and Class members did not receive the benefit of their bargain with Defendants and were injured as described in detail herein.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

93. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

94. Defendants have received and retained a benefit from Plaintiffs and members of the Class, resulting in inequity.

95. Defendants benefitted through their unjust conduct by profiting from selling services that required Plaintiffs and the Class members to provide valuable PII without providing adequate data security for that PII.

96. Plaintiffs and the Class members conferred a benefit on Defendants when they purchased services from Defendants and provided Defendants with their PII and payment information.

97. Defendants failed to provide Plaintiffs and the Class with full compensation in exchange for their PII, which Defendants obtained through inequitable means because Defendants failed to disclose their inadequate data security practices.

98. It is inequitable for Defendants to retain these benefits.

99. This claim is pled in the alternative in the event Plaintiffs and the Class members do not have an adequate remedy at law.

100. As a result of Defendants' inequitable conduct, the amount of their unjust enrichment should be disgorged, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150
(On Behalf of the California Subclass)

101. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

102. Defendants violated § 1798.150 of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiffs' and Class members' unencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

103. Defendants collect consumers' personal information as defined in Cal. Civ. Code § 1798.140. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As identified herein, Defendants failed to do so. As a direct and proximate result of Defendants' acts, Plaintiffs' and the Class members' personal information, including unencrypted names, account numbers, Social Security numbers, driver's license numbers, and dates of birth, was subjected to unauthorized access, and exfiltration, and theft.

104. Plaintiffs and the Class members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold customers' PII, including Plaintiffs' and the Class members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

105. On October 1, 2020, Plaintiffs' Counsel sent a notice letter to Defendants' registered service agents via FedEx Priority Overnight. Assuming Defendants cannot cure the Data Breach within 30 days, and Plaintiffs believe any such cure is not possible under these facts and circumstances, then Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

SEVENTH CAUSE OF ACTION
Violation of the California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of the Plaintiffs and the California Subclass)

106. Plaintiffs incorporate by reference and reasserts all previous paragraphs.

107. Defendants engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.*

108. As alleged herein, Defendants engaged in the following unlawful and unfair conduct: (i) negligence; (ii) negligence *per se* (iii) breach of implied contract; and (iv) breach of express contract; and (v) violation of the CCPA.

109. As also alleged herein, Plaintiffs and Class members were directly and proximately harmed in several ways as a result of Defendants' unlawful and/or unfair conduct. Defendants are liable to Plaintiffs and Class members for those damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class as requested herein;

b. Appointing Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendants engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendants' conduct and requiring Defendants to implement proper data security practices;

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: October 2, 2020

/s/Karen Hanson Riebel

Karen Hanson Riebel (MN # 0219770)
Kate M. Baxter-Kauf (MN # 392037)
Maureen Kane Berg (MN # 033344X)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
mkberg@locklaw.com

Gayle M. Blatt, *Pro Hac Vice* forthcoming
Jeremy Robinson, *Pro Hac Vice* forthcoming
P. Camille Guerra, *Pro Hac Vice* forthcoming
James M. Davis, *Pro Hac Vice forthcoming*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com
jrobinson@cglaw.com
camille@cglaw.com
jdavis@cglaw.com

Attorneys for Plaintiffs and the Class